Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claims 1-18. (canceled)

19. (currently amended) A group signature device for providing a message (m) accompanied by a group signature (S), comprising:

means for storing personalized data (z, Kz) identifying a member (M) of a group (G); ~~and~~

encryption means (B3) for producing an encrypted text (C), intended to be associated with said message (m), using said personalized data (z, Kz);

signing means (B6) for producing the group signature (S) with a private signature key (SK) common to all group members using the message to be signed (m) and said encrypted text (C); and

~~means for producing the group signature (S) using the message (m) and the personalized data (z, Kz) such that a checker, upon receiving the message (m) accompanied by the group signature (S), is able to verify that the message (m) is associated with the group (G) based on the personalized data (z, Kz) and the group signature (S), to authenticate the message (m) with the identity of the member (M) of the group (G) remaining anonymous to the checker; and~~

means for outputting the message (m) and the group signature (S) to ~~the~~ a checker, such that the checker, upon receiving the message accompanied by the group signature, is able to verify that the message (m) is associated with the group (G)

based on the group signature (S), with the identity of the member (M) of the group (G) remaining anonymous to the checker.

Claim 20. (canceled)

21. (currently amended) A group signature device according to claim [[20]] 19, further comprising:

means (B5) for combining the message (m) to be signed and the encrypted text (C) ~~associated with said message (m)~~ in the form of a concatenation of the message (m) with the encrypted text (C).

Claim 22. (canceled)

23. (currently amended) A group signature device according to claim [[20]] 19, wherein

said personalized data is an identifier (z) personal to the member (M);

said means for storing further includes an encryption key (K) common to all members of the group (G); and

encryption means (B3) produces said encrypted text (C) using the identifier (z) and said encryption key (K).

24. (previously presented) A group signature device according to claim 23, in which encryption means (B3) produces said encrypted text (C) using the identifier (z) and a random number (r).

25. (currently amended) A group signature device according to claim [[20]] 19, wherein

said personalized data is a diversified encryption key (Kz) specific to each member (M) of the group (G); and

encryption means (B3) produces said encrypted text (C) using at least one data and said diversified encryption key (Kz).

26. (currently amended) A group signature device according to claim 25, wherein said at least one data includes a random number (r).

27. (currently amended) A group signature device according to claim [[24]] 19, wherein the encryption means (B3) uses a secret key ~~(K) and the Advanced Encryption Standard (AES) public~~ encryption algorithm.

28. (currently amended) A group signature device according to claim [[26]] 19, wherein the encryption means (B3) uses one of the Rivest, Shamir, Adleman (RSA) public key encryption algorithm or the Advanced Encryption Standard (AES) secret key ~~public~~ encryption algorithm[[s]].

29. (currently amended) A group signature device according to claim [[22]] 19, wherein the ~~signature~~ signing means (~~Sig~~-B6) uses a private key signature algorithm (SK).

30. (previously presented) A group signature device according to claim 29, in which the private key signature algorithm is of the Rivest, Shamir, Adleman (RSA) type.

31. (previously presented) A group signature device according to claim 19, in which said group signature device is a portable communicating device.

32. (previously presented) A group signature device according to claim 31, in which said portable communicating device is a smart card.

33. (currently amended) A method for secure communication of message (m) sent by a member (M) of a group (G) using a group signature (S), said method comprising:

producing the group signature (S) of the message (m) by signing, with a private signature key (SK) common to all group members, a set including the message (m) and encrypted text (C) produced by using a personalized data (Z, Kz); and ~~(M) of the group (G);~~

~~integrating personalized data (z; KZ) into the message (m); and~~

outputting the message (m) along with the group signature (S)~~; and~~

~~verifying that the message (m) is associated with the group (G) based on the personalized data (z, Kz) and the group signature (S) to authenticate the message (m) without identifying the member (M) of the group (G)~~.

34. (currently amended) The method according to claim 33, further comprising:

~~in which said~~ verifying, by ~~is performed~~ using a public key (PK) corresponding to said private signature key (SK), that the message (m) is associated with the group (G) based on the group signature (S), without identifying the member (M) of the group (G).

35. (currently amended) The method according to claim 33, further comprising the steps of:

decrypting the encrypted text (C) thus obtaining the ~~making correspondence data between the identities of members (M) of the group (G) and their~~ personalized data (z, Kz); and ~~available, before said producing the group signature(S);~~

~~decrypting the personalized data received from an electronic device for which the group signature (S) is to be opened; and~~

~~opening the group signature (S) if the decrypted personalized data corresponds to the identity of~~ identifying the member (M) of the group (G) based on said personalized data (z, Kz).

36. (currently amended) The method of claim 35, further comprising ~~the steps consisting of~~:

producing a private signature key (SK) common to all members of group (G);

producing personalized data (z, Kz) identifying the member (M) accepted into the group (G); ~~associated with said electronic device to be personalized;~~ and

registering said personalized data (z, Kz) with ~~a~~ the private signature key (SK) in an electronic device personalized to said member (M) of the group (G) ~~contained in said electronic device~~.

Claims 37-38. (canceled)

39. (currently amended) A group signature system for ensuring a secure communication of ~~authenticating~~ a message (m) sent by a member (M) of ~~accompanied by~~ a group (G) using a group signature (S), said group signature system comprising:

an electronic device configured to store a personalized data (z, Kz) identifying the [[a]] member (M) of the [[a]] group (G), to produce an encrypted text (C) intended to be associated with said message (m) using said ~~the group signature (S) using the message (m) and the~~ personalized data (z, Kz), and to produce the group signature (S) with a private signature key (SK) common to all group members using ~~output~~ the message (m) and said encrypted text (C), and to output the message (m) and the group signature (S);

a checker that receives the message (m) accompanied by the group signature (S) output from the electronic device, said checker being configured to verify that the message (m) is associated with the group (G) based on the ~~personalized data (z, Kz) and the~~ group signature (S), the identity of the member (M) remaining anonymous to the checker; and

a trusted authority configured to identify the member (M) of the group (G).

Claim 40. (canceled)